ACDIS Occasional Paper

The Past Perfect Promise of Facial Recognition Technology

Kelly Gates
Institute of Communications Research
University of Illinois at Urbana-Champaign

Research of the Program in Arms Control, Disarmament, and International Security

University of Illinois at Urbana–Champaign

June 2004

This publication is supported by funding from the University of Illinois and is produced by the Program in Arms Control, Disarmament, and International Security at the University of Illinois at Urbana-Champaign.

ACDIS Publication Series: ACDIS *Swords and Ploughshares* is the quarterly bulletin of ACDIS and publishes scholarly articles for a general audience. The ACDIS *Occasional Paper* series is the principal publication to circulate the research and analytical results of faculty and students associated with ACDIS. The ACDIS *Research Reports* series publishes the results of grant and contract research and technical reports. Publications of ACDIS are available upon request. For additional information consult the ACDIS home page on the World Wide Web at: http://www.acdis.uiuc.edu/

Published 2004 by ACDIS//ACDIS GAT:1.2004
University of Illinois at Urbana–Champaign
359 Armory Building, 505 E. Armory Ave.
Champaign, IL 61820-6237

Series editor: Matthew A. Rosenstein
Copy editor: Lydia Allen

The Past Perfect Promise of Facial Recognition Technology

Kelly Gates

Institute of Communications Research
University of Illinois at Urbana-Champaign

Program in Arms Control, Disarmament, and International Security
University of Illinois at Urbana-Champaign
June 2004

ABOUT THE AUTHOR

Kelly Gates is a Ph.D. candidate in the Institute of Communications Research at the University of Illinois at Urbana-Champaign. Beginning in September 2004, she will be an Assistant Professor in the Department of Media Studies at the City University of New York, Queens College. She holds a bachelor's degree in Advertising from Penn State University and a master's degree in Mass Communication from Miami University of Ohio. Gates has just completed her dissertation on "Our Biometric Future: The Social Construction of an Emerging Information Technology." She has published articles in *Television and New Media* and *Information, Theory and Society*. The work for this *Occasional Paper* was completed when she was serving as a Thesis Initiation Fellow at the Program in Arms Control, Disarmament, and International Security in 2003.

INTRODUCTION

> *Of all the dramatic images to emerge in the hours and days following the September 11 attacks, one of the most haunting was a frame from a surveillance-camera video capturing the face of suspected hijacker Mohamed Atta as he passed through an airport metal detector in Portland, ME. Even more chilling to many security experts is the fact that, had the right technology been in place, an image like that might have helped avert the attacks. According to experts, face recognition technology that's already commercially available could have instantly checked the image against photos of suspected terrorists on file with the FBI and other authorities. If a match had been made, the system could have sounded the alarm before the suspect boarded his flight.*[1]

The idea that computerized face recognition might have helped avert the al-Qaeda terrorist attacks was perhaps the most ambitious claim circulating about biometric identification technologies in the aftermath of September 11. Along with the enormous flood of imagery of the day, relayed in the news media were the out-of-focus surveillance-camera images of two of the alleged attackers. The recorded video image from the airport in Portland, Maine that appears to show Mohammad Atta and Abdulaziz Alomari passing through airport security is a familiar part of 9/11 iconography. And it is virtually impossible to reference this image without also invoking the claim that facial recognition technology could have identified the men in the image as wanted terrorist suspects. Already existing commercially available technology, according to this regretful yet strangely hopeful assertion, "could have instantly checked the image against photos of suspected terrorists." Technologies that use digital readings of the face to identify individuals could have saved the United States from the worst terrorist attack in its history.

The precise origin of the claim is hard to identify; it seemed to spring forth simultaneously from multiple sources. If it first came from a biometrics industry representative, such as oft-quoted Visionics Chief Eecutive Officer Joseph Atick, it was quickly embraced and repeated by other public voices who felt sure it was true.[2] This hopeful, regretful possibility was the basis for hearings held on Capitol Hill following September 11. On November 14, 2001, the Technology, Terrorism and Government Information Subcommittee of the Senate Judiciary Committee held a hearing on "Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism." In her opening remarks, Senator Dianne Feinstein (Democrat-California) asked, "How could a large group of coordinated terrorists operate for more than a year in the United States without being detected, and then get on four different airliners in a single morning without being stopped?" The answer, she noted, "is that we could not identify them." Voicing again the assertion that had become part of the repertoire of public responses to the 9/11 events, she asserted, "In the case of at least two of the hijackers authorities had pictures of them as suspects prior to the attack, and airport cameras actually photographed them. But because these cameras didn't use facial biometric systems, security was not alerted and the hijackers remained free to carry out their bloody plans."

The idea that the events of 9/11 could have been prevented with the sophisticated technological products of modernity is laden with what Pat Gill has called "technostalgia"—the desire to revise the past to re-determine the present, while at the same time admitting the impossibility of this endeavor.[3] The claim might be said to embody a collective psychological need to believe that the nation was not as vulnerable as it appeared, that our technological sophistication remains unscathed and in fact would have stopped the men had it been in place. This technostalgic longing to revise the past provides a paradoxical sort of origin myth for facial recognition technology. In the post-9/11 context, the technology emerges as an already existing, reliable and hi-tech solution to the newest, most pressing problem facing the nation. This move effectively erases the history of these technologies, even as it inserts them fully formed into the past. What is effectively erased is the fact that well before 9/11, a whole set of social actors were engaged in ongoing struggles and negotiations over the development and deployment of this technology. While it was not already fully formed and ready to identify the nation's post-cold war enemy Other, it *was* already "embedded in and shaped by a rich web of cultural practices and ideas."[4]

This paper will begin to explore this rich web of cultural practices and ideas, examining facial recognition technology in the pre-9/11 world.[5] Following Raymond Williams and other scholars studying the historical

emergence of media technologies, my aim here is to restore *intention* to the process of research and development of facial recognition technology.[6] This effort requires rescuing it from post-9/11 technostalgic narratives and recapturing some of its history. I discuss late nineteenth-century ancestors to biometrics, early research on machine recognition of faces in the 1960s, and the growing state and private interest in the technology during the 1990s. The early emergence of face recognition as part of the state surveillance apparatus and as marketed, commercially available products takes place in the post-Soviet/post-cold war decade of the 1990s. Its arrival on the scene happens alongside and in relation to the spread of the Internet and computer networking, neoliberal economic policies like the North Atlantic Free Trade Agreement and the 1996 Telecomm Act, and the enormously publicized public-private competition to map the human genome, creating a universal digital representation of human essence. Biometrics embody a digital mode of representing the body, and techniques of digitalization are enlisted to lay a particular claim to truth about the relationship between the body and identity.[7] The aim is to automate the process of connecting bodies to identities, and in some cases, to distribute that identified body across computer networks for specific purposes; namely, to control *access*—access to the benefits of citizenship, to the national territory, to information, to computer networks themselves, to transportation systems, and to specific spaces of consumption and safety. Facial recognition and biometrics must be located firmly within their historical and cultural context of emergence, with particular attention to the ways these technologies are being enlisted both symbolically and programmatically in the effort to reproduce and redefine the nation-state (namely the United States) and its considerable authority in the post-cold war, post-9/11 period.[8]

PART ONE
Late Nineteenth-Century Bodily Identification Systems

In order to understand how and why computerized facial recognition has become both a possibility and perceived necessity, it helps to consider the problem of identification in historical perspective. In *The Origins of Totalitarianism*, Hanna Arendt argued that the claim to authority for determining who belongs and who does not is a central component of sovereignty.[9] The identification of subjects residing within or attempting to enter state territories has been a particular preoccupation of modern states. Since their emergence out of traditional societies, modern states have necessarily invested considerable effort in defining their membership—those individuals who are entitled to state benefits and protections and subject to state controls. The rise of a culture of identification, in which individuals are assigned official identities and routinely asked to verify those identities in social and economic exchanges, corresponds to the expansion of the modern state. Identifying citizens and distinguishing them from non-citizens emerged as an essential function of the modern state, one that required the construction of "state memory" as a complex of archives, records, documents, administrative procedures and human agents.[10]

The state and other institutions have faced and consistently attempted to address a complex of problems in their ongoing efforts to construct systems for accurately and reliably identifying individual constituents at key points of contact. One enduring problem has been that of articulating identity to the body in a consistent and reliable way. The seemingly natural connection between the body and identity of the person reveals itself to be in perpetual slippage, a never-ending mirror stage of development where identity never precisely occupies the body or vice versa. The hybridity of both identity and the body, and their instability over time, make their accurate, reliable articulation that much more difficult, even with the most cooperative subjects and the most precise renderings or descriptions of identity. Technologies, such as identification documents, have been designed to facilitate identification by binding identity to the body, often by incorporating other technologies, such as photographs and signatures, and through practices associated with law, for example, the legal requirement to carry passports for international travel.[11] However, documents have always been insufficient to the task, incapable of definitively and reliably assigning identities to specific bodies. Jane Caplan explains a similar problem in terms of the mediated nature of "self-sameness," referring to "the tension between 'identity' as the *self-same*, in an individualizing, subjective sense, and 'identity' as *sameness with another*, in a classifying, objective sense.[12] According to Caplan, the identification document functions as

> the portable token of an originary act of bureaucratic recognition of the "authentic object"—an "accurate description" of the bearer recognized and signed by an accredited official, and available for repeated acts of probative ratification. The experience of self-sameness is thus *never unmediated*, either subjectively or objectively; it operates through a system of signs and recognitions that intrudes alterity into the heart of identity. *This is the critical tension at the heart of a culture of identification*.[13]

Biometrics represent the latest attempt to solve this eternal, ultimately unsolvable problem: the inescapable *mediation of identity.*

A second problem—and one that has been clearly and consistently targeted in the effort to improve and perfect identification systems—has been the fallibility of the human agents or workers operating within identification systems, both in terms of their cultural prejudices and lack of objectivity, as well as their inability to manage the amount of information required to individuate bodies and identities. Human agents of identification, such as police and immigration officers, necessarily draw on their own subjective perceptions and preconceived notions about individual types to identify or verify identities, a process seen as fraught with error and inefficiency. The proposed solutions to this so-called problem of human fallibility have frequently involved delegation of responsibility for identification to technologies, including letters, printed documents, bodily measurements, photographic portraiture, archival systems, and administrative procedures—a leap of faith based on the problematic assumption that technologies are neutral and separable from the messiness of human social agents. Each successive technology of identification is constructed as more scientific, and hence more neutral, than those that preceded it.

A third enduring problem has been the enormity of the archival and administrative effort necessary to achieve universal identification, especially given the hybridity of populations and their perpetually changing

compositions. The task of identifying each individual consistently and reliably across time and space has been a difficult one even with the most static of populations, and as subject populations grow in size they inevitably complicate systems of identification such that controlling individual identities becomes an enormous bureaucratic challenge for even the most organized and informationalized apparatus.

Biometrics are not the first technical effort to connect bodies to identities. Several key nineteenth-century developments in identification systems evidence a perceived need to use the body itself as a marker of identity at this time of modern state expansion. These included the application of photography for identification purposes, the relatively short-lived and sporadically applied method of anthropometry, and the much more successful and enduring scientific method of dactyloscopy, or fingerprinting. While these efforts to devise identification systems were motivated by the problem of identifying criminals and criminal recidivists, the imperative to identify criminals, and the systems elaborated to do so, overlapped with systematic state efforts to identify and distinguish between citizens and non-citizens. In the United States as elsewhere, fear of criminals and fear of foreigners blended into one another, particularly as "nativists" stereotyped immigrants as inherently criminal.[14] According to Caplan and Torpey, "Police practices in the [late nineteenth and early twentieth centuries] asserted a more specialized domain of authority over criminal identification and detection, which became a crucial site for further identificatory and supervisory developments that were then reappropriated into universal systems of civil identification.[15] This is not to say that identification systems were deployed universally for the identification of all citizens; while such projects were certainly conceived, such a massive undertaking likely would have exceeded the administrative capacities (and interests) of the state. Still, systems devised for criminal identification, including photography, anthropometry, and dactyloscopy, were employed in various contexts for identifying entrants to state territory; they lent themselves to targeted procedures for the identification outside the realm of criminal identification, strictly defined.

Photographic portraiture was enlisted to address the identification imperative from its very inception, and this use of the photographic medium shaped both its development and cultural significance. Photographic portraiture carried with it utopian visions about the possibilities of its realist representational capacity. Its emergence coincided and interacted with the growing professionalization of policing and the introduction of "expert" sciences into the work of law enforcement. Authorities clearly saw it as a potential solution to the problem of binding identities to bodies and compensating for the fallibility of human agents of identification systems. The value of photographs for the purposes of identification was realized very early by the British police, who began employing photographers for such purposes in the 1840s.[16] Although "the photograph's status as evidence and record (like its status as Art) had to be produced and negotiated," the leap of realism (not to mention speed) that it achieved over artists' portraits surely was difficult to contest.[17] It was a medium uniquely suited to truth-production. According to John Tagg, photography's power to evoke truth resulted not only from the privilege that industrial societies attached to mechanical means, but also from the way that a new and more penetrating form of the state mobilized it as part of a complex of emerging state apparatuses. The emerging disciplinary institutions incorporated photography as part of sophisticated new surveillance techniques that generated a new kind of detailed and productive knowledge about the subjects being observed. Tagg inserts photography into the Foucauldian historical analysis of discipline and outlines the "striking rendezvous" that occurred between the growth of photographic records and the growth of the state, especially the formalized police apparatus.[18] The disciplinary method relied on both the individual portrait of the criminal—the body made object—and the accumulated images organized into filing systems. Individuation involved not only the "turning of real lives into writing," as Foucault elaborated, but also into images that could be meticulously examined one-by-one, and accumulated into filing systems, amounting to a new representation of society.[19] Still, though it represented a promising new technique of identification and continues to serve as a constitutive component of identification systems, photography alone had limitations in terms of its capacity to definitively connect bodies to identities and to compensate for the inadequacies of human perception. It created new administrative and archival problems, necessitating new procedures, areas of expertise, and bodily classification schemes.

Anthropometry represents a particularly noteworthy precursor to biometrics because it involved both standardized bodily measurements and sophisticated archival and retrieval systems. As examined extensively by scholars like Alan Sekula, Martine Kaluszyski, and Anne Joseph, the science and system of anthropometry was used sporadically by emerging police and state programs for the identification of criminals and other "undesirables."[20] Developed by Alphonse Bertillon in France in the 1880s, anthropometry involved the meticulous measurement and description of individual bodies, records that were then stored in archives

according to a highly organized system that allowed for easy retrieval. According to Sekula, the central artifact of Bertillon's system was not the camera but the filing cabinet, a "bureaucratic-clerical-statistical system of 'intelligence.'"[21] Bertillon's anthropometry involved not just measuring and documenting faces and bodies, but also classifying those measurements and documents according to an intricate scheme that allowed for more efficient retrieval, a necessity for effective identification and a precursor to the computerized and networked database. The archive promised to provide "a standard physiognomic gauge of the criminal" and to "assign each criminal body a relative and quantitative position with a larger ensemble."[22] There was a considerable effort on the part of its proponents to invest anthropometry with legitimacy, and to position it as a credible, scientific solution to criminal recidivism and other problems of identification—problems that the expanding modern state was beginning to address in systematic ways. Though short-lived and only sporadically applied, Bertillon's was the first rigorous system for archiving and retrieving identity, projects that became central to the state's administrative apparatus.[23]

Other innovative actors conceptualized systems for coding and distributing the identified body across existing information networks in order to extend the state's authority to define its citizens and territorial control. Matt Matsuda describes two systems developed by early twentieth-century doctors in France for transforming bodies into coded numerical references and circulating those references as a system of signals via telegraph.[24] Dr. A. Motet's method involved "attributing to each individual physical feature…a classifying number based on the recognized elements most characteristic of their physical person, and inscribed in some ways upon their organ."[25] Anthropometric measurements, physical descriptions, and photographic portraiture would be translated into reference codes for easy distribution across telegraph networks for the purposes of identifying vagabonds and other problematic identities. While such a system was never fully institutionalized, it was clearly conceptualized well before computerization, digitization, and electronic information networks provided new possibilities and new areas of need for storing and distributing representational forms of bodies and their corresponding identities. Computerized forms of bodily identification are in many ways consistent with these earlier state efforts, and similarly tied to cultural preoccupations with constructing the limits and possibilities of the nation-state.

PART TWO
Early Research on Machine Recognition of Faces

Biometrics are the newest innovation in identification systems. Today, there are a variety of commercially available technologies that are designed to read the body as a marker of identity: facial recognition as well as digital fingerprinting, hand geometry, voice recognition, and iris and retina scanning. Other automated systems for identifying humans that have not hit the market include gait and smell-based technologies. DNA typing is used in criminal identification, and the Federal Bureau of Investigation has developed the Combined DNA Index System (CODIS) for networking local DNA databanks on a national scale, but a DNA profile still takes several weeks to generate, so DNA biometrics cannot be applied as yet for "real-time" identification. To say that biometrics "read the body as a marker of identity" is itself a way of placing these technologies in a black box, summing up how they work in oversimplified, metaphoric terms. Like other forms of biometrics, automated facial recognition enlists many technologies and processes, including photography and video, computer algorithms and digitalization, feature extraction, image compression, computer matching, and electronic data storage. Teaching the computer how to "see" a face has been no simple accomplishment. As two prominent Massachusetts Institute for Technology (MIT) facial recognition researchers noted in the early nineties, "developing a computational model of face recognition is quite difficult, because faces are complex, multidimensional, and meaningful visual stimuli."[26] Automated facial recognition has involved research in a number of scientific areas, including computer vision, image processing and analysis, pattern recognition, and statistics.[27]

Some of the earliest research on machine recognition of faces can be traced back to the 1960s at a company called Panoramic Research, Inc. in Palo Alto, California, one of many companies springing up in California at the time to conduct research in what was later termed artificial intelligence. The work at Panoramic Research was funded largely by the US Department of Defense and various intelligence agencies, and thus was unavoidably entrenched in the US fight for cold war technological dominance.[28] Research on machine recognition of faces was conducted by a man named Woodrow Wilson "Woody" Bledsoe, one of the co-founders of Panoramic Research. Bledsoe is now widely recognized as one of the early researchers of artificial intelligence and a pioneer in the field of automated reasoning. A member of the Army Core of Engineers during World War II and a devout Mormon, he was a firm believer in incremental scientific advances as opposed to major leaps or paradigm shifts.[29] The technique Bledsoe developed was dubbed "man-machine facial recognition." Drawing on his earlier work on computer recognition of letters, it involved manually entering into a computer the positions of facial feature points in an image, a process known as "feature extraction." A human operator would use a "rand tablet" to extract the coordinates of features such as the corners of the eyes and mouth, the top of the nose, and the hairline or point of a widows peak.[30] The name of the person in an image was stored in a database along with facial coordinates, and records were classified based on those measurements. The computer was then prompted to identify the name of the closest test image, given a set of distances between facial feature points. Bledsoe was apparently very proud of this painstaking research on machine recognition of faces; however, very little of it was published because the funding was provided by an unnamed intelligence agency that did not allow much publicity.[31] In 1966, Bledsoe left Panoramic Research to return to academia as a Professor of Mathematics at University of Texas-Austin. His work on machine recognition of faces was continued at Stanford Research Institute.

The earliest work to successfully program a computer to confirm the existence or absence of a face in an image, without human operator intervention, was published in *Pattern Recognition* in 1969 by Sakai, Nagao, and Fujibayashi.[32] Then in 1970, M. D. Kelly produced a landmark dissertation project on face recognition at Stanford. His technique enabled the computer to automatically extract the head and body outlines from an image and then locate the eyes, nose, and mouth, using three images of each individual: an image of the body, an image of the background without the body, and a close-up image of the head.[33] In 1973, Takeo Kanade's dissertation research at Kyoto University in Japan reported the same results using only a photograph of the face and a new "flexible picture analysis scheme" that consisted of a collection of simple "subroutines," each of which worked on a specific part of the picture. Kanade's project correctly identified fifteen out of twenty people.[34] The effort to automate the process of human face recognition was underway by the 1970s, but it clearly had far to go before machines could achieve the same capacity as human beings for recognizing faces

and connecting them to names. The personal computer itself had yet to become a staple in middle class American homes when researchers were envisioning and working on the automated identification of people by machines. The computer would need the capacity to see, and especially to see and discern individual human beings, if it could ever achieve "intelligent" status.

Intelligent Machines and Machine-Like Intelligence

The effort to build intelligent machines and facilitate human-machine intelligent interaction has been a motivating force for scientists developing algorithms and other techniques for automated facial recognition. Along the way, scientists studying face recognition began to recognize and consistently comment on the remarkable capacity that humans have for recognizing faces. The effort to program computers to identify human faces led to an increased awareness of the complexity of the process, so that an admiration of the human capacity for face recognition and a desire to simulate it in computerized form came to inspire and inform the research. In a special issue of the *Journal of Cognitive Neuroscience* devoted to both human and machine recognition of faces, two scientists at MIT's Media Lab noted,

> The human ability to recognize faces is remarkable. We can recognize thousands of faces learned throughout our lifetime and identify similar faces at a glance even after years of separation. This skill is quite robust, despite large changes in the visual stimulus due to viewing conditions, expression, aging, and distractions such as glasses or hairstyle or facial hair.[35]

Not only were computer scientists taken with humans' robust face perception skills, they also displayed an apparent interest in using computational models to explain or better understand how the human brain performs this complex operation. In the same journal issue, a scientist at Harvard University's Division of Applied Science expressed his hope "that current attempts to build computer vision face recognition systems will shed light on how humans perform this task and the difficulties they overcome."[36]

In feedback loop fashion, the study of human face perception in cognitive science influenced research in machine face recognition, and computational models of face recognition were used to devise theories to explain how humans perceived and recognized faces. As Haugeland has noted, the term *cognitive science* does not refer to every theory of cognition, "but only to those sharing a certain broad outlook—which is sometimes called the 'information processing' or 'symbol manipulation' approach."[37] Artificial intelligence is, in a sense, the "distilled essence of cognitive science."[38] The cognitive sciences emerged in the United States in the 1940s along with cybernetics and information theory, and further developed in the latter half of the 1950s, as scientists conceptualized the notion of artificial intelligence and interpreted the workings of the brain as a data processing system.[39] If technical articles on automated facial recognition are any indication, the emergence of this technology must be understood in relation to the interplay of ideas between the fields of cognitive science and artificial intelligence.

While researchers studying machine recognition of faces have generally understood that it would be impossible to develop technology that mimics the way the human brain recognizes faces, they nevertheless have looked to research in the fields of psychophysics and neuroscience for guidance in solving, or at least thinking about, difficult technical problems. Relevant research in these fields has included work examining whether face recognition is a dedicated process, whether face perception is the result of holistic or feature analysis, and the relative importance of various facial features for human recognition of faces. The use of both global and local features for representing and recognizing faces in certain automated recognition systems has drawn on research suggesting that the human brain operates in such a way when it analyzes a face. Other questions that are considered relevant to development of automated recognition concern how children recognize faces, what role facial expressions play in recognition, the role of race and gender, and our ability to recognize faces in images of varying quality.[40] In addition, automated facial recognition has been partly guided by research in neuropsychology, suggesting that the brain processes identities and expressions using functionally distinct neurological pathways, and that the relative lightness and darkness of areas of the face play a role in our assessment of human face representations.[41]

PART THREE
Intensified Research Interest and Commercialization in the 1990s

Research on facial recognition and other computerized forms of bodily identification continued throughout the 1970s and '80s at Bell Labs and at Stanford and other major research universities, but it was the 1990s that saw a veritable explosion of research interest, along with commercialization and the integration of prototypes into existing real-world identification systems.[42] Researchers made advances in efforts at programming computers to locate a face in an image, to segment the face from background clutter, and to extract facial features. Increasing amounts of computing power facilitated faster techniques and accommodated larger, higher quality images, in greater quantities. Computerization and the spread of information networks provided both the possibility and the areas of need for new identification technologies. Documents like passports and driver's licenses, which had always had their shortcomings, were seen as increasingly inadequate to the task of identification across networks. The banking, credit card, and telecommunications industries were among those social actors expressing an interest in technologies that could give them greater control over transactions and information networks. In addition, employers of all sorts saw the need to monitor and control their employees' access to both computer networks and to the physical space of the workplace.

The transfer of the technology from the lab to real-world applications came along with the development of the "eigenface" technique at the MIT Media Laboratory, and a technique called local feature analysis (LFA) developed at the Computational Neuroscience Lab at Rockefeller University.[43] These techniques refer to the actual process of digitizing the face and matching it against another image or set of images: the recognition process. The recognition process actually follows techniques of face *detection*, or finding a face in an image, and *segmentation*, or extracting a face from the background, themselves challenging problems in the field of computer vision. After a face is located as an image and segmented from the background, an algorithm or set of computer instructions translates the extracted face image into a digital code or template that is then searched against a database of images (one-to-many matching), *or* matched against an image or template that have been stored on a machine-readable identification document (one-to-one matching).

A heavily cited article on the eigenface technique was published by MIT researchers Matthew Turk and Alex Pentland in 1991 in the *Journal of Cognitive Neuroscience*.[44] As the authors explain, the eigenface technique (from the German prefix *eigen*, which means "own" or "individual") relies on composite grayscale facial representations derived from a database of images. The eigenface technique automatically reconstructs new faces by combining features from the composites. As MIT scientists describe the process:

> The scheme is based on an information theory approach that decomposes face images into a small set of characteristic feature images called "eigenfaces," which may be thought of as the principal components of the initial training set of face images. Recognition is performed by projecting a new image into the subspace spanned by the eigenfaces ("face space") and then classifying the face by comparing its position in face space with the positions of known individuals.[45]

Automated face recognition here occurs in the virtual world of "face space," where face images are "decomposed" to reveal their informational essence, classified and compared in a digital form to produce matches that can then be interpreted by human operators. Eigenfaces are ghostly looking face images that researchers describe as the most efficient way to encode the face, bearing an uncanny resemblance to the criminal composites of the famous nineteenth-century eugenicist Frances Galton. Image features used in the eigenface technique need not correspond to our intuitive notions of facial features, the MIT researchers explain, but the process does ostensibly resemble human face perception in that recognition occurs quickly using a representation of the whole face. In addition, "relatively small changes cause the recognition to degrade gracefully" while abrupt changes in facial appearance cause recognition to fail, as occurs with humans. According to Turk and Pentland, the eigenface technique is not an "elegant" but a "practical" solution to the problem of computer face recognition.[46]

A second technique, local feature analysis, extracts features of the face from an image, classifies them individually, and creates a template based on the sizes of facial geographic patterns and the distances between them.

The *Identity* of Facial Recognition Technology

By the mid 1990s, a number of researchers studying facial recognition had remade themselves as entrepreneurs, hoping to ride the information technology (IT) economic boom. They formed new companies, dedicated to marketing facial recognition products. Visionics Corporation, Viisage Technology, and Miros Inc. emerged as the most promising, attracting modest venture capital as well as grants from federal government agencies. Intense competition among new facial recognition vendors took the form of inflated claims about the capabilities of the products, as well as consistent boasting about the superb scientific credentials of company representatives. Visionics Corporation was formed by three researchers from the Computational Neuroscience Lab at Rockefeller University. The head of the lab, a man named Atick, became CEO of the company. Atick was a bit of an overachiever, writing a 600-page physics textbook at age fifteen and earning a Ph.D. in mathematical physics from Stanford after having been accepted into graduate school there as a sixteen-year-old.[47] He became interested in how the brain processes visual information, how to apply those theories to computer algorithms, and how to transform that science into marketable technologies. Atick and his colleagues developed their facial recognition product using the LFA technique, which they also developed. They named their product "FaceIt®" and spun it as an "Enabling Technology with Mass Appeal."

In the names given to the technology and the slogans used to sell it, one can begin to discern the construction of a cultural identity for automated facial recognition. The name "FaceIt," for example (always accompanied in print by the trademark symbol "®"), has circulated in news reporting and other public discourse as an identifying term for the Visionics facial recognition product; though it is not quite a household word, it is one of the more prominent product names associated with the technology. A loaded signifier and curious identifier for the technology, the term "FaceIt" begs consideration of its cultural signification. Reading "It" as an acronym, "FaceIt" can be interpreted in rather straightforward terms as a variation of "Face IT," short for "face information technology" or "face identification technology." Read as an immediate address, "FaceIt" suggests that subjects should literally face the technology, or face the camera, so that their bodies can be identified. On a connotative level, the phrase "face it" signifies a demand to "face facts" or accept the truth, which begs the question as to what facts or truth are being asserted. Are we being asked to accept the technology's authority to accurately articulate identity to the body? Should we face the inevitability of the technology's application by the state and other institutional users, and the potential erosion of civil liberties in the name of security or convenience? Perhaps "it" is a hopeful reference to a utopian technological future that should be embraced rather than resisted. Of course, we can never know exactly what facts we should accept, since the pronoun "it" is without a referent. In this sense it seems to point to or inspire generalized insecurities and uncertainties about the present or the future, precisely the justifications or necessity for new and improved surveillance and identification technology. "FaceIt" is the just the sort of meaningless phrase that George Orwell might have taken to task in "Politics and the English Language," or incorporated into the fictional newspeak vocabulary as shorthand for a more complex statement no longer accessible. The obvious Orwellian underpinnings of "FaceIt" make it a curious and almost consciously ironic choice to identify a facial recognition technology.

The slogan "Enabling Technology with Mass Appeal" is similarly ironic and without actors, referents, or subjects. Exactly *what* does "FaceIt" enable, and to what "mass" does it appeal? The adjective "enabling" signifies making something possible; that which enables lends agency to something or someone else. Of course, there is no precise subject being enabled by the technology in this phrase, so it could just as easily mean enabling the state to track one's movement, or enabling an organization to monitor their employees' workday. The technology ostensibly enables other technologies to function in specific ways; for example, the company claims that FaceIt® makes "passive" closed-circuit television systems more "active" by automatically scanning video feeds, extracting faces, converting them into digital templates, and searching them against a "watch list" database. In this sense, it promises to "enable" more effective use of closed-circuit television (CCTV) systems and improved practices for state and private security agencies that employ them. The other odd choice of terms in the sales slogan—"mass appeal"—evokes an image of hordes of people clamoring to use the technology. Such an image detracts from the idea of *individual* identification, since a "mass" is the opposite of specific individuals. It seems to sell the technology more to investors interested in rising stock prices than to potential institutional users interested in accurately identifying their individual constituents among the masses. Ironically, "mass appeal" also signifies manipulation and control, leaving an appropriate if unintentional impression.

The Post-Cold War "Unidentifiable" Enemy

Regardless of the effectiveness of the marketing techniques, clear areas of need for facial recognition came into focus in the 1990s for one of the technology's early adopters: the national security state.[48] A new concept was fueling research interests and programs: the decidedly post-cold war concept of "asymmetric threats." This concept is briefly addressed in a promotional video for the Defense Advanced Research Projects Agency (DARPA), the central research and development organization for the US Department of Defense.[49] The video opens with a montage of images and sounds representing the cold war, the fall of the Berlin Wall, and the new US security threats of the 1990s. Black and white images of Soviet soldiers marching in file are followed by color images of Arab men, still photos of individuals, then a video image of a large group of Arab-looking men moving rhythmically en masse. The montage is accompanied by the following voice-over narration:

During the cold war, the enemy was predictable, identifiable, and consistent. We knew the threats, the targets were clear. But times change. Today, with the demise of the other superpower, America is in a different position: a position of vulnerability. When the enemy strikes, it isn't predictable. It isn't identifiable. It is anything but consistent. Times change. We are in a world of "asymmetrics," and we need transformational solutions. The asymmetric threat is now a reality of global life. How do we detect it? How do we predict it? How do we prevent it?[50]

This opening sequence encapsulates the post-cold war identity crisis of the national security state. The text invokes a nostalgic longing for the so-called predictability and consistency of the cold war, when the enemy was ostensibly well defined and *identifiable*. This nostalgic idea of an identifiable enemy is used to define a new form of national "vulnerability"—the construction of "America" as "vulnerable" precisely because the nation cannot identify its enemy, literally or symbolically. The assumption is that the United States is more vulnerable than ever, that the "asymmetric threats" facing the nation today are even greater than the perpetual threat of nuclear holocaust during the forty-year cold war. Although it is not difficult to poke holes in this rhetoric (especially since the United States never did fight a clearly defined and identifiable enemy in any of the cold war wars), this is truly a vulnerability for the national security state, which in fact *must* define and identify an enemy in order to legitimate itself. The notion of "asymmetric threats" becomes a key construction in the effort to justify and reproduce an imperial-sized national security state. The United States may no longer have an enemy that can match its military might, according to this message, but it has many small enemies that represent significant threats, disproportionate to their small size and military resources. These "unidentifiable" and "unpredictable" enemies are constructed as major risks, a construction given considerable leverage by the enormity of the violence on 9/11.

However, as the video demonstrates, the state *has* clearly identified the post-cold war enemy Other. The first image in the montage is the destroyed Khobar Towers US Military Barracks in Saudi Arabia bombed in 1996 allegedly by Saudi members of Hezbollah (along with plenty of US finger-pointing at Iran). The only image to appear twice in the first minute of the video, it is a defining image and a defining moment for the national security state in its effort to reconstruct itself both symbolically and programmatically in the post-cold war context. When it appears a second time, the image serves as the backdrop to a series of mug shot images of terrorist suspects. Most of the images represent Arab-looking men, with the exception of one man of ambiguous race, and the series of mug shots concludes with image of Osama bin Laden, now the archetypal Arab "face of terror." (The video was made after 9/11.) Thus the notion of an "unidentifiable" enemy referenced in the voiceover narration stands out against the visual images of specific, clearly identified and racialized brown bodies.

The construction of an unidentifiable enemy—which is in fact clearly identified as the racialized Arab Other—functions to legitimate both the technologies and the reproduction of the national security state in the post-cold war context. The problem of the unidentifiable enemy also works to dehistoricize and decontextualize facial recognition technology, reifying it as a so-called hi-tech solution to the problems of security and terrorism (themselves reified concepts). Further, positioning the technology as national security solution justifies its use for any means necessary, supporting the application of the technology not only to identify the purported unidentifiable enemy, but also as part of the ongoing effort to manage and control "the everyday individuality of everybody," a project decidedly central to modern forms of state and disciplinary power.[51]

The erasure of the muddy history of facial recognition technology in post-9/11 technostalgic claims has accommodated the young biometric industry's rhetoric of scientific neutrality, and their effort to secure the authority and desirability of their product. The hi-tech, scientific image so critical to the industry's efforts to sell their technologies relies in part on the dissociation of the biometrics from the struggles and negotiations involved in their early development, as well as the ongoing social and technical challenges that they face. These challenges detract from the image of the technology as scientific and "state-of-the-art," revealing the extent to which these new bodily identification systems are enmeshed in the politics and preoccupations of interested actors. The very notion of "hi-tech" or "state-of-the-art" necessarily involves the reification of that which is labeled hi-tech; a faith or belief in the hi-tech inescapably involves committing the error of mistaking an abstraction for a material thing.

The emergence of automated facial recognition as a security technology must be understood not only as part of post-9/11 security hysteria, but also in relation to the profound post-cold war identity crisis of the national security state. The post-9/11 technostalgic assertions made by Senator Feinstein and others not only efface the technology's muddy history and reify automated facial recognition as "hi-tech," they also frame the problem of security as one of recognition or identification, the need to accurately and reliably identify the enemy Other. While this framing enabled the biometrics industry to capitalize on the hyper-paranoia of the post-9/11 moment, the preoccupation of the national security state with identifying new enemies and problems to legitimate itself intensified a decade earlier, following the fall of the Berlin Wall and the break up of the Soviet Union. A 1991 political cartoon captured well the emerging identity crisis of the post-cold war national security state. It depicted a bloated Uncle Sam loaded down with ballistic missiles and other accoutrements of industrial warfare, along with the caption, "All dressed up with no one to fight." During the 1990s, the state adapted information technology to the effort of identifying new enemies, a necessary effort to justify the reproduction of the enormous and enormously expensive cold war security apparatus. The new geopolitical context would not allow for the identification of one red menace or villainous nation-state, only many smaller villains that were ostensibly more difficult to locate, define, and identify. New bodily identification technologies would lend themselves to the effort to identify the post-cold war enemy other, or more paradoxically, these technologies would justify themselves with reference to allegedly unidentifiable "asymmetric threats." Part of the process of identifying a new enemy in a decade of computerization, digitalization, and proliferating information networks involved making that enemy newly identifiable through informationalized means, while in fact identifying specific (types of) individuals as threats based in part on rhetorical allusions to their *un*identifiability.

As David Lyon has argued, the "deeper shifts" toward intensified surveillance practices were already in process before 9/11; the attacks "served simply to accelerate their arrival in a more public way."[52] The national security state *did* envision integrating biometrics into terrorist identification systems before September 11, 2001, and the industry marketed the technology partly in terms of this potential application. This line of marketing allowed the industry to immediately position the technologies as a solution to the problem of terrorism in the days following the attacks. The notion of security through identification—specifically through the binding of bodies to identities in a consistent, reliable, "hi-tech" way—was already formulated and ready to be considered as a logical solution to the new problem of catastrophic foreign terrorism on US soil.

Notes

[1] Alexandra Stikeman, "The Technology Review; Top Ten: Biometrics," *Technology Review* (January/February 2001), http://www.technologyreview.com/magazine/jan01/print_version/tr10_atick0101.asp (accessed December 13, 2001).
[2] Visionics Corporation is now Identix, Inc. (Visionics and Identix merged in 1992).
[3] Pat Gill, "Technostalgia: Making the Future Past Perfect," *Camera Obscura: A Journal of Feminism, Culture and Media Studies* 40 (1997): 163-179.
[4] Susan Douglas, *Inventing American Broadcasting, 1899-1922* (Baltimore, MD: Johns Hopkins University Press, 1987), xv.

[5] I submitted my dissertation proposal on September 10, 2001. My plan for the original project was to examine the use of biometrics in three different contexts: in urban spaces, in the workplace, and at the border. The project was unavoidably transformed by the explosion of attention biometrics received in the aftermath of September 11, which led me to abandon the workplace as a site of concentrated focus in the interest of manageability. This paper is an effort to recapture the pre-9/11 aura of the technology—the meanings it held and the problems it was being envisioned to solve before the terrorist attacks reframed the discourse surrounding these technologies so that they became, first and foremost, "homeland security" technologies, solutions to the new problems of foreign, catastrophic terrorism on United States soil.

[6] Raymond Williams, *Television: Technology and Cultural Form* (New York: Schoken Books, 1975).

[7] According to Irma van der Ploeg, "Biometrics and the Body as Information: Normative Issues of the Socio-Technical Coding of the Body" in *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination,* ed. David Lyon, (New York: Routledge, 2003), 57-73, it is important to consider "how the translation of (aspects of) our physical existence into digital code and 'information,' and the new uses of bodies this subsequently allows, amounts to a change on the level of ontology, instead of merely that of representation" (59). She argues that biometrics, genetics, and other technologies for digitizing the body signal the emergence of a new *ontology* of the body, rather than merely new ways of representing or defining the body. This new ontology of the body redefines and reworks the body as information flows and communication patterns, and is quite distinct from the familiar anatomical-physiological ontology of the body, itself a late eighteenth-century historical construction that altered the meaning and experience of embodiment through its gradual incorporation into the institutional practices of medicine, law, education, public policy, etc. The "informatization" and digitization of the body through biometrics, genetics, biomedical, visualization and other technologies are not merely defining the same body with new language. They may substantively reconfigure bodies and have real effects at the level of embodiment. "The notion of body ontology enables us to describe the way the human body is implicated in a process of co-evolution with technology—information technologies, but also surgical, chemical and genetic and visualization techniques, and combinations of these" (64).

[8] There are a variety of commercially available technologies designed to "digitize" the body in order to read it as an identification document, store it in a database, and distribute it across information networks. The now familiar list of biometric technologies includes not only facial recognition, but also digital fingerprinting, hand geometry, iris and retina scanning, and voice recognition. Here I focus on facial recognition technology precisely because the "content" of the medium—the image of the human face—carries such social and cultural significance, and because of the considerable sway this particular biometric technology has come to have in the public imagination. However, in order to understand the historical emergence of facial recognition technology, it is necessary to consider it in isolation from other biometric technologies. When I use the term "biometrics," I mean to generalize across the range of identification technologies that use digitized readings of the body as the basis of identifying individuals. Conversely, when I use the term "facial recognition" I mean to specify this unique type of biometric that aims to mimic one of the primary, visual ways that humans recognize each other, and a technique that promises to identify humans with their direct interface with an identification system.

[9] Hanna Arendt, *The Origins of Totalitarianism* (New York: Harcourt Brace Jovanovich, 1973), 284.

[10] Matt K. Matsuda, *The Memory of the Modern* (New York: Oxford University Press, 1996) and Pamela Sankar, *State Power and Record-Keeping: The History of Individualized Surveillance in the United States, 1790-1935* (Ph.D. Dissertation, University of Pennsylvania, 1992).

[11] While driver's licenses may technically function to authorize the bearer to operate a car, in fact they are equally functional for managing mobility.

[12] Jane Caplan and John Torpey, eds., *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton, NJ: Princeton University Press, 2001), 51, her emphasis.

[13] Ibid., my emphasis.

[14] Simon Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Cambridge, MA: Harvard University Press, 2001).

[15] Caplan and Torpey, *Documenting Individual Identity*, 9.

[16] John Tagg, *The Burden of Representation* (London: Macmillan, 1987), 75.

[17] Ibid., 6.

[18] Ibid.

[19] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (New York: Vintage Books, 1977), 192.

[20] Alan Sekula, "The Body and the Archive," *October* 39 (1986): 3-64; Martine Kaluszynski, "Republican Identity: Bertillonage as Government Technique," in Caplan and Torpey, *Documenting Individual Identity,* 123-138; Anne Joseph, "Anthropometry, the Police Expert, and the Deptford Murders: The Contested Introduction of Fingerprinting for the Identification of Criminals in Late Victorian and Edwardian Britain," in Caplan and Torpey *Documenting Individual Identity,* 164-183.

[21] Sekula, "The Body and the Archive," 16.

[22] Ibid., 17.

[23] Ibid.

[24] Matsuda, *The Memory of the Modern*.
[25] Ibid., 138.
[26] Matthew Turk and Alex Pentland, "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience* 3, no.1 (1991): 71-86.
[27] Rama Chellappa, Charles L. Wilson, and Saad Sirohey, "Human and Machine Recognition of Faces: A Survey," *Proceedings of the IEEE* 83, no. 5 (May 1995): 705-740.
[28] As Manuel De Landa, *War in the Age of Intelligent Machines* (New York: Zone Books, 1991) has noted, "Artificial intelligence has been a product of post-Sputnik American military research. The specific balance of power between DARPA [the Defense Advanced Research Projects Agency] and other Cold War think tanks (e.g., ONR, RAND, etc.), the paramilitary agencies trying to monopolize cutting-edge computer research (the NSA, for instance) and centers for corporate research (IBM, DEC, etc.) formed the environment wherein modern computers evolved" (176-177).
[29] Michael Ballantyne, Robert Boyer, and Larry Hines, "Woody Bledsoe: His Life and Legacy," *AI Magazine* 17, no. 1 (Spring 1996): 7-20.
[30] Ibid.
[31] Ibid.
[32] T. Sakai, M. Nagao, and S. Fujibayashi, "Line Extraction and Pattern Recognition in a Photograph," *Pattern Recognition* 1 (1969): 233-248.
[33] M.D. Kelly, "Visual Identification of People by Computer," Technical Report AI-130, Stanford AI Project, Stanford, CA, 1970.
[34] Takeo Kanade, Picture Processing System by Computer Complex and Recognition of Human Faces, Doctoral Dissertation, Department of Computer Science, Kyoto University, Kyoto, Japan, 1973. Published as T. Kanade, *Computer Recognition of Human Faces* (Basel, Stuttgart: Birkhauser, 1977).
[35] Turk and Pentland, "Eigenfaces for Recognition," 71.
[36] Alan Yuille, "Deformable Templates for Face Recognition," *Journal of Cognitive Neuroscience* 3, no. 1 (1991): 59-70.
[37] John Haugeland, "Semantic Engines: An Introduction to Mind Design," in *Mind Design: Philosophy, Psychology, Artificial Intelligence*, ed. John Haugeland (Cambridge, MA: MIT Press, 1981): 1-34.
[38] Ibid., 2.
[39] Armand Mattelart and Michele Mattelart, *Theories of Communication: An Introduction* (Thousand Oaks, CA: Sage, 1998), 133-134.
[40] Chellappa et al., "Human and Machine Recognition," 710-711.
[41] Vicki Bruce, Peter J.B. Hancock, and Mike Burton, "Human Face Perception and Identification," in Harry Wechsler et al. (eds.), *Face Recognition: From Theory to Applications* (Berlin: Springer, 1998), 51-72.
[42] Chellappa et al., "Human and Machine Recognition."
[43] Turk and Pentland, "Eigenfaces for Recognition." Viisage Technology uses the eigenface method for their FaceEXPLORER and other facial recognition products.
[44] The article was published in a special issue on face perception that included articles on monkey, human, and machine recognition of faces. The monkey and human investigations were concerned with what regions of the brain process faces, and a disease called prosopagnosia, a neurological syndrome that makes humans incapable of recognizing faces.
[45] Turk and Pentland, "Eigenfaces for Recognition," 72.
[46] Ibid.
[47] Stikeman, "The Technology Review."
[48] Similar needs for automated identification from video surveillance were expressed by local law enforcement agencies and private security companies. The 1990s saw an explosion of visual information generated by rapidly proliferating closed-circuit television systems. Police and private security firms in both the United States and Europe (especially the United Kingdom) were installing thousands of CCTV systems for monitoring urban centers, banks, gated communities, workplaces, and capital-intensive "territories of consumption" such as malls and casinos. Police and private security actors saw the need to automate surveillance video systems, in large part to control the labor costs of monitoring these systems. Thus emerged the notion of "Smart CCTV"—the integration of facial recognition technology with video surveillance. This is the application that ostensibly would have prevented 9/11, according to Senator Feinstein and other voices endorsing the technology in the wake of the attacks. The police in the London Borough of Newham implemented one of the first publicized applications of "Smart CCTV" in 1998, using the Visionics FaceIt® system, later followed by systems in Tampa, Florida and Virginia Beach.
[49] In the United States, federal agencies such as the Department of Defense and the National Institute of Justice have provided funding to universities and private companies for research and development of facial recognition technology. Following the bombing of the Khobar Towers US military barracks in Saudi Arabia in 1996, DARPA began to develop a program initially called "Image Understanding Force Protection" (IUFP). This program would provide funding to universities and private companies for research and development on multi-modal biometric technologies for identifying humans at a distance (without their actual cooperation or direct interface with the identification system). By "multi-modal" they mean using and combining multiple biometrics in one system, including facial, voice, gait, and other forms of

automated identification. The program was later renamed "Human ID at a Distance," and was recently placed under the auspices of DARPA's controversial "Total Information Awareness" program, headed by John Poindexter. Visionics Corporation has been among the recipients of Human ID funding, receiving two million dollars from DARPA in 2001, and one million dollars each in 2002 and 2003, to improve upon their FaceIt® facial recognition product (Visionics has merged with and is now called Identix, Inc.). Viisage Technology has also received funding to develop their eigenface-based facial recognition systems through the Human ID program, and more recently was awarded a grant of $4.1 million from the DoD's Technical Support Working Group. Universities that have received funding through the Human ID program include; Carnegie Mellon, University of Maryland, Columbia University, University of Southampton, University of Texas-Dallas, Colorado State University, University of South Florida, and Georgia Tech. These actors, and the technology itself, have been enlisted in the effort to secure US military installations abroad, especially in the Middle East.

[50] Video shown by Dr. Robert L. Popp, Deputy Director, Information Awareness Office, Defense Advanced Research Projects Agency, as part of his Keynote Address to the Biometrics Consortium Conference, September 23, 2002, Arlington, VA.

[51] Foucault, *Discipline and Punish*, 191.

[52] David Lyon, *Surveillance after September 11* (Malden, MA: Polity Press, 2003).